JOURNAL OF NUMBER THEORY 52, 69–84 (1995)

Hensel's Lemma and the Divisibility by Primes of Stirling-like Numbers

FRANCIS CLARKE*, †

Department of Mathematics, University College of Swansea, Swansea, SA2 8PP Wales

Communicated by Alan C. Woods

Received June 16, 1993; revised August 10, 1993

We prove a version of Hensel's Lemma which applies to analytic functions on the p-adic integers. This is used to obtain results on the divisibility of Stirling numbers of the second kind which generalise results of Davis.

INTRODUCTION

Divisibility properties of the Stirling numbers of the second kind have been studied in, for example, [19, 25, 23, 20, 9, 17]. Congruences amongst the Stirling numbers have been considered in [3, 4, 6, 22, 15, 12, 13, 26]. Various results in algebraic topology involve the arithmetic of Stirling numbers; see [18, 6, 8].

If p is a prime let

$$T_p(n, k) = \sum_{\substack{j=0 \\ p \nmid j}}^{k} (-1)^{k-j} \binom{k}{j} j^n.$$

In [9], Davis gave a method for calculating the exponent of the prime 2 in $T_2(n, 5)$ and $T_2(n, 6)$. His paper includes calculations which enable one to compute these exponents for $n < 2^{100}$. In this paper we show how his results generalise to give the divisibility of $T_p(n, k)$ by p for other primes p and other values of k. The essential idea is the observation that Davis' rather ad hoc technique is in fact an application of Hensel's Lemma, i.e., the Newton–Raphson method for finding zeros of differentiable functions in the p-adic context.

* I thank Don Davis for sending me an early version of his paper [9] and for some helpful comments on this work.

† E-mail address: F.Clarke@Swansea.ac.uk.

0022-314X/95 $6.00

The numbers $T_p(n,k)$ are "Stirling-like" in the following sense. By Stirling's formula (see Sect. 5.1 of [7])

$$k!\,S(n,k) = \sum_{j=1}^{k} (-1)^{k-j} \binom{k}{j} j^n,$$

where $S(n,k)$ is the Stirling number of the second kind. Thus $k!\,S(n,k) - T_p(n,k)$ is divisible at least by p^n. In this sense, $T_p(n,k)$ is a good p-adic approximation to $k!\,S(n,k)$. Apart from a sign, our notation follows Lundell [20, 19], who refers to $T_p(n,k)$ as a "partial Stirling number". We conjecture, see Sect. 5, that for all primes p, if $n \geqslant k$, then $v_p(k!\,S(n,k)) = v_p(T_p(n,k))$. Our calculations show that, for the values of k and p which are considered in Sections 3 and 4, this holds when $n < p^{100}$, and suggest very strongly that the conjecture is true for all $n \geqslant k$.

The precise results on the divisibility of $T_p(n,k)$ depend very much on k and p, but the general framework is as follows. Let $v_p(x)$ denote the exponent of the prime p in x. We show how to obtain a p-adic integer u and an integer q such that for n in a residue class modulo $p^j(p-1)$, for some j, $v_p(T_p(n,k)) = q + v_p(n-u)$. Detailed calculations are carried out for $p=2$ with $k \leqslant 7$, and for $p=3$ with $k \leqslant 5$.

In applying Hensel's Lemma the functions for which we have to find p-adic zeros are not polynomial functions, while Hensel's Lemma is normally stated for polynomials; see for example, Proposition 2 of Chap. 2 of [16] or Theorem 3 of Chap. 1 of [14]. Thus in Section 1 we show how to extend Hensel's Lemma to analytic functions of a p-adic variable. In [1] Amice gives a general form of Hensel's Lemma for analytic functions, but her results do not provide the estimates which we need for the case of a simple p-adic zero.

We show in Proposition 2 how to estimate the p-adic valuation of an analytic function near a zero. It is this result, together with the ability to evaluate the zeros, which gives rise to our results on the divisibility of $T_p(n,k)$. In Section 2 we explain how to extract analytic functions from the partial Stirling number $T_p(n,k)$ and prove some results about p-adic logarithms which are needed for the estimates necessary to apply Hensel's Lemma. In Sections 3 and 4 we perform explicit calculations for the primes 2 and 3, respectively. In Section 5 we discuss the consequences for the divisibility of the Stirling numbers themselves, which are summarised in Theorem 9. An Appendix gives a table of the first 50 digits of the p-adic zeros found in Sections 3 and 4.

1. Hensel's Lemma for Analytic Functions

By Hensel's Lemma we understand the application of the Newton–Raphson method in the p-adic context. Over the real numbers one sees by

looking at the quadratic form of Taylor's theorem that the rate of convergence of Newton's method depends on the size of the second derivative. Taylor's theorem for polynomials is, of course, a purely algebraic result; see, for example, Sect. 30, Théorème 4 of [10]. That Hensel's Lemma for integer polynomials does not involve estimating the size of the second derivative depends on the fact that for an integer polynomial the remainder term in Taylor's theorem is an integer polynomial, and so being integer valued on the integers has supremum norm at most 1.

It is clear that for a general p-adically analytic function the method will work but we should not expect such a uniform result as in the polynomial case. In the absence of the Mean Value Theorem the situation is slightly more subtle over the p-adic integers than over $\mathbf{R}$. The version of Hensel's Lemma which we will prove essentially involves an estimate of the second derivative. We shall see in the examples in Sections 3 and 4 that the estimate involved can, in certain cases, be quite easily calculated.

It is natural to ask whether the requirement of analyticity is necessary. It is in fact sufficient to require the function to be strictly twice differentiable in the sense of [2, 27]. However since this approach leads to more intractable estimates and all the functions which occur in our applications are (piecewise) analytic we have not pursued this direction here.

Let $\mathbf{Q}_p$ denote the field of p-adic numbers equipped with the valuation $|x|$, normalised so that $|p| = 1/p$. We write $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x| \leqslant 1\}$ for the ring of p-adic integers.

Suppose that $c \in \mathbf{Z}_p$ and that $f : c + p^k \mathbf{Z}_p \to \mathbf{Q}_p$ is analytic in the sense that $x \mapsto f(c + p^k x)$ is an analytic function on $\mathbf{Z}_p$; see Sect. 4 of Chap. 14 of [21]. Then for $x \in c + p^k \mathbf{Z}_p$ and $h \in p^k \mathbf{Z}_p$ we have

$$f(x+h) = f(x) + hf'(x) + h^2 \frac{f''(x)}{2!} + \cdots,$$

so that

$$f(x+h) = f(x) + hf'(x) + h^2 g(x, h), \tag{1}$$

for some continuous function $g : (c + p^k \mathbf{Z}_p) \times p^k \mathbf{Z}_p \to \mathbf{Q}_p$ such that $g(x, h) \to f''(x)/2$ as $h \to 0$. Since g is continuous it is bounded. Thus there exists $r \in \mathbf{Z}$ such that $|g(x, h)| \leqslant p^r$ for all x and h.

PROPOSITION 1. *With the preceding notation, if $u \in c + p^k \mathbf{Z}_p$ is such that*

$$|f(u)| < \min\left(\frac{|f'(u)|}{p^{k-1}}, \frac{|f'(u)|^2}{p^r}\right),$$

then there exists $v \in c + p^k \mathbf{Z}_p$ such that $|f(v)| < |f(u)|$.

Proof. Note that it is implicit in the hypotheses that $f'(u) \neq 0$. Let $v = u + h$, where $h = -f(u)/f'(u)$. Then, by (1), $f(v) = h^2 g(u, h)$ as long as $h \in p^k \mathbf{Z}_p$. This is guaranteed since $|f(u)| \leqslant |f'(u)|/p^k$. Now

$$|f(v)| = |h|^2 \, |g(u, h)| \leqslant \frac{p^r \, |f(u)|}{|f'(u)|^2} \, |f(u)| < |f(u)|,$$

completing the proof.

Now $f'(x)$ is a continuous function of x so there exists $s \geqslant k - 1$ such that $|f'(u + h)| = |f'(u)|$ for all h such that $|h| < 1/p^s$. It follows that if

$$|f(u)| < \min\left(\frac{|f'(u)|}{p^s}, \frac{|f'(u)|^2}{p^r}\right), \tag{2}$$

then the number v constructed in the proof of Proposition 1 satisfies $|f'(v)| = |f'(u)|$. Hence the hypotheses of Proposition 1 hold for v. Thus we can iterate the method, obtaining a Cauchy sequence of values converging to a p-adic zero of $f(x)$. The next result gives a formula for $|f(x)|$ near such a zero; its corollary shows that the zero is isolated.

PROPOSITION 2. *Suppose that $f(u) = 0$, and that r is the integer defined above, so that $|(f(x + h) - f(x) - hf'(x))/h^2| \leqslant p^r$ for all $x \in c + p^k \mathbf{Z}_p$ and $h \in p^k \mathbf{Z}_p$. Then for all $v \in c + p^k \mathbf{Z}_p$ such that $|v - u| < |f'(u)|/p^r$ we have $|f(v)| = |v - u| \, |f'(u)|$.*

Proof. Suppose that $h = v - u$. Then (1) gives $f(v) = h(f'(u) + hg(u, h))$. But if $|h| < |f'(u)|/p^r$, then $|hg(u, h)| < |f'(u)|$ so that $|f'(u) + hg(u, h)| = |f'(u)|$.

COROLLARY 3. *If $f(u) = 0$ and $f'(u) \neq 0$, then $f(v) \neq 0$ for all $v \in c + p^k \mathbf{Z}_p$ with $v \neq u$ such that $|v - u| < |f'(u)|/p^r$.*

In practice one may not wish, or be able, to compute $f(u)$ and $f'(u)$ exactly. One is much more likely to have access to a finite initial segment of their p-adic expansions. This is, however, no obstacle to applying the Hensel's Lemma technique to find a zero of f to any required accuracy. For it is easy to see that in the proof of Proposition 1 the rôle of h may be played by any $\tilde{h}$ such that $|\tilde{h} + f(u)/f'(u)| < |f(u)/f'(u)|$.

To be specific, suppose that the hypotheses of Proposition 1 hold and that $|f(u)| = 1/p^i$ and $|f'(u)| = 1/p^j$, with $f(u) \equiv p^i y \bmod p^{i+1}$ and $f'(u) \equiv p^j z \bmod p^{j+1}$, where y and z belong to $\{1, 2, \ldots, p - 1\}$. Then $v = u - p^{i-j} y \bar{z}$ will satisfy $|f(v)| < |f(u)|$, where $z\bar{z} \equiv 1 \bmod p$. Moreover if $i > j + s$ our remarks above show that $f'(v) \equiv f'(u) \bmod p^{j+1}$ and we can use the same value $\bar{z}$ each time that we iterate the procedure. This approach will, however, reduce the rate of convergence.

2. Partial Stirling Numbers and p-adic Logarithms

Recall that if p is a prime we define the partial Stirling number $T_p(n, k)$ by

$$T_p(n, k) = \sum_{\substack{1 \leq j \leq k \\ j \not\equiv 0 \bmod p}} (-1)^{k-j} \binom{k}{j} j^n.$$

If p is an odd prime and we fix an integer a, with $0 \leq a < p-1$, then there is an analytic function $f_{a,k}: \mathbf{Z}_p \to \mathbf{Z}_p$ such that $f_{a,k}(m) = T_p(a + m(p-1), k)$ for all non-negative integers m; see Sect. 5 of Chap. 14 of [21]. Thus we may write

$$f_{a,k}(x) = \sum_{\substack{1 \leq j \leq k \\ j \not\equiv 0 \bmod p}} (-1)^{k-j} \binom{k}{j} j^a (j^{p-1})^x.$$

If $p = 2$ the situation is slightly different. The function $f_{0,k}$ is infinitely differentiable, but it is not analytic on $\mathbf{Z}_2$, unless $k \leq 2$. However its restriction to each of $2\mathbf{Z}_2$ and $1 + 2\mathbf{Z}_2$ is analytic; see Section 5 of Chap. 14 of [21].

We will study the p-divisibility of $T_p(n, k)$ by means of the p-adic interpolations $f_{a,k}(x)$. By Strassmann's Theorem [24] (see also Theorem 4.1 of Chap. 4 of [5]) $f_{a,k}(x)$ has only a finite number of zeros $u_1, u_2, \ldots, u_N$ in $\mathbf{Z}_p$. For the simple zeros we can use the results of Section 1 to evaluate them, and then Proposition 2 will provide a result of the form $|f_{a,k}(x)| = |x - u_i|\,|f'_{a,k}(u_i)|$ for x sufficiently close to u_i.

We have

$$f'_{a,k}(x) = \sum_{\substack{2 \leq j \leq k \\ j \not\equiv 0 \bmod p}} (-1)^{k-j} \binom{k}{j} j^a (j^{p-1})^x L(j^{p-1}),$$

where $L(y)$ is the p-adic logarithm, which may be defined when $|y - 1| < 1$ by the series

$$L(y) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(y-1)^n}{n}; \tag{3}$$

see Sect. 5 of Chap. 14 of [21].

To obtain the estimates necessary to apply Propositions 1 and 2 to the functions $f_{a,k}(x)$ we need to know $|L(y)|$.

Proposition 4. (1) *If p is an odd prime, or if $p = 2$ and $|y - 1| < \frac{1}{2}$, then $|L(y)| = |y - 1|$, and if $|y - 1| = 1/p^k$, then $L(y) \equiv y - 1 \bmod p^{k+1}$.*

(2) *If $p = 2$ and $|y - 1| = \frac{1}{2}$, then $|L(y)| = |y + 1|$.*

Proof. The first case follows immediately from the series (3) defining $L(y)$ since the first term has a larger valuation than any of the others. For the second case we use the fact that since $L(y)$ is the derivative at 0 of the function $x \mapsto y^x$ we have

$$L(y) = \lim_{i \to \infty} \frac{y^{2^i} - 1}{2^i}.$$

Suppose that $|y-1| = \frac{1}{2}$ and $|y+1| = 1/2^k$. Then $|y^2 - 1| = 1/2^{k+1}$, i.e., $y^2 \equiv 1 + 2^{k+1} \bmod 2^{k+2}$. It follows by induction that $y^{2^i} \equiv 1 + 2^{k+i} \bmod 2^{k+i+1}$, for $i \geqslant 1$, and so

$$\frac{y^{2^i} - 1}{2^i} \equiv 2^k \bmod 2^{k+1},$$

which gives the required result.

For certain calculations in Sections 3 and 4 we shall need to know various logarithmic values more accurately. We can compute these values by a method similar to that used in the proof of part (2) of Proposition 4.

PROPOSITION 5. (1) *If p is an odd prime and if $|y-1| = 1/p^k$ with $k > 0$, then, for all $n \geqslant 2k$,*

$$L(y) \equiv \frac{y^{p^{n-2k}} - 1}{p^{n-2k}} \qquad \bmod p^n.$$

(2) *For $p = 2$, if $|L(y)| = 1/2^k$ with $k > 1$, then, for all $n \geqslant 2k-1$ if $|y-1| < \frac{1}{2}$, and for all $n \geqslant 2k$ if $|y-1| = \frac{1}{2}$,*

$$L(y) \equiv \frac{y^{2^{n-2k+1}} - 1}{2^{n-2k+1}} \qquad \bmod 2^n.$$

Proof. For the case of an odd prime, let $r = n - 2k$. Since $y \equiv 1 \bmod p^k$ it follows that $y^{p^r} \equiv 1 \bmod p^{k+r}$. Write $y^{p^r} = 1 + Ap^{k+r}$. Then

$$\begin{aligned} y^{p^{r+1}} &= (1 + Ap^{k+r})^p \\ &= 1 + Ap^{k+r+1} + \binom{p}{2} A^2 p^{2k+2r} + \cdots \\ &\equiv 1 + Ap^{k+r+1} \qquad \bmod p^{2k+2r+1}, \end{aligned}$$

and inductively $y^{p^{r+i}} \equiv 1 + Ap^{k+r+i} \bmod p^{2k+2r+i}$, for all $i \geqslant 0$.

Thus $(y^{p^{r+i}} - 1)/p^{r+i} \equiv Ap^k \bmod p^n$, for all $i \geqslant 0$. The result follows since $L(y) = \lim_{i \to \infty} (y^{p^i} - 1)/p^i$.

In the case where $p=2$, the congruence $y^{2^r} \equiv 1 \bmod 2^{k+r}$ holds for $r \geqslant 0$ if $|y-1| < \frac{1}{2}$, and for $r \geqslant 1$ if $|y-1| = \frac{1}{2}$. If we let $r = n-2k+1$ and $y^{2^r} = 1 + A2^{k+r}$, then

$$\begin{aligned} y^{2^{r+1}} &= (1 + A2^{k+r})^2 \\ &= 1 + A2^{k+r+1} + A^2 2^{2k+2r} \\ &\equiv 1 + A2^{k+r+1} \qquad \bmod 2^{2k+2r}, \end{aligned}$$

and inductively $y^{2^{r+i}} \equiv 1 + A2^{k+r+i} \bmod 2^{2k+2r+i-1}$, i.e., modulo 2^{n+r+i}, for all $i \geqslant 0$. The result now follows as in case (1).

If $f(x) = f_{a,k}(x)$ in Eq. (1), and we write $g_{a,k}(x, h)$ for the corresponding function denoted by $g(x, h)$ in Section 1, then we have

$$g_{a,k}(x,h) = \sum_{\substack{2 \leqslant j \leqslant k \\ j \not\equiv 0 \bmod p}} (-1)^{k-j} \binom{k}{j} j^a (j^{p-1})^x \frac{(j^{p-1})^h - 1 - hL(j^{p-1})}{h^2}.$$

We will need the following result in estimating $|g_{a,k}(x, h)|$.

LEMMA 6. *If* $|y-1| < 1$ *and* $h \in \mathbf{Z}_p$, *with* $|h| < 1$ *if* $p = 2$ *and* $|y-1| = \frac{1}{2}$, *or if* $p = 3$ *and* $|y-1| = \frac{1}{3}$, *then*

$$\left| \frac{y^h - 1 - hL(y)}{h^2} \right| = \begin{cases} |y-1|^2, & \text{if } p \text{ is odd,} \\ 2\,|y-1|^2, & \text{if } p=2 \text{ and } |y-1| < \frac{1}{2}, \\ 2\,|y+1|^2, & \text{if } p=2 \text{ and } |y-1| = \frac{1}{2}. \end{cases}$$

Proof. The conditions ensure that we may write

$$y^h = 1 + hL(y) + \frac{h^2 L(y)^2}{2!} + \frac{h^3 L(y)^3}{3!} + \cdots.$$

Thus

$$\frac{y^h - 1 - hL(y)}{h^2} = \frac{L(y)^2}{2}\left(1 + \frac{hL(y)}{3} + \frac{h^2 L(y)^2}{12} + \cdots\right).$$

Now since $|L(y)| < 1$, with $|L(y)| < \frac{1}{2}$ if $p = 2$, the factor $1 + hL(y)/3 + h^2 L(y)^2/12 + \cdots$ is a unit so that the result follows using the formula for $|L(y)|$ given in Proposition 4.

The following more precise estimate follows from the previous proof.

COROLLARY 7. *With the assumptions of Lemma* 6, *if* $|h| = 1/p^j$ *and* $|L(y)| = 1/p^k$, *then*

$$\frac{y^h - 1 - hL(y)}{h^2} \equiv \frac{L(y)^2}{2} \mod \begin{cases} p^{j+3k}, & \text{if } p > 3, \\ p^{j+3k-1}, & \text{if } p = 2 \text{ or } p = 3. \end{cases}$$

3. EXPLICIT CALCULATIONS WITH $p = 2$

For the prime 2 the first interesting case is $k = 5$; see [9]. We have $T_2(n, 5) = f_{0,5}(n)$, with $f_{0,5}(x) = 5 + 10 \cdot 3^x + 5^x$, so that $f'_{0,5}(x) = 10 \cdot 3^x L(3) + 5^x L(5)$. Since $|L(3)| = |L(5)| = \frac{1}{4}$ by Proposition 4, and $|3^x| = |5^x| = 1$, it follows that $|f'_{0,5}(x)| = \frac{1}{4}$ for all $x \in \mathbf{Z}_2$. It follows easily from Lemma 6 that $|g_{0,5}(x, h)| = \frac{1}{8}$ if $h \in 2\mathbf{Z}_2$.

Now $f_{0,5}$ is analytic on $2\mathbf{Z}_2$. Since $|f_{0,5}(0)| = \frac{1}{16}$ it follows from Proposition 1 and Corollary 3 that there exists a unique $u_0 \in 2\mathbf{Z}_2$ such that $f_{0,5}(u_0) = 0$. Proposition 2 shows that $|f_{0,5}(x)| = |x - u_0|/4$ for all $x \in 2\mathbf{Z}_2$. Similarly there is a unique zero u_1 of $f_{0,5}$ in $1 + 2\mathbf{Z}_2$, with $|f_{0,5}(x)| = |x - u_1|/4$ for all $x \in 1 + 2\mathbf{Z}_2$. The first 100 binary digits of u_0 and u_1 are given in [9], where they were evaluated by a method equivalent to the application of Hensel's Lemma.

The case $k = 6$ is similar. We have $f_{0,6}(x) = -6 - 20 \cdot 3^x - 6 \cdot 5^x$. It is easy to see that $|f'_{0,6}(x)| = \frac{1}{8}$ and $|g_{0,6}(x, h)| = \frac{1}{16}$ for any $x \in \mathbf{Z}_2$ and $h \in 2\mathbf{Z}_2$; the analysis is exactly the same as in the $k = 5$ case. Again [9] contains the beginning of the 2-adic expansion of the two zeros involved.

For $k = 7$ we need to work a little harder. We have $f_{0,7}(x) = 7 + 35 \cdot 3^x + 21 \cdot 5^x + 7^x$ so that $f'_{0,7}(x) = 35 \cdot 3^x L(3) + 21 \cdot 5^x L(5) + 7^x L(7)$.

Now Proposition 4 gives $|L(3)| = |L(5)| = \frac{1}{4}$ and $|L(7)| = \frac{1}{8}$. However to evaluate $|f'_{0,7}(x)|$ we shall need $L(3)$, $L(5)$ and $L(7)$ modulo 64. Proposition 5 gives $L(3) \equiv 52 \bmod 64$, $L(5) \equiv 60 \bmod 64$ and $L(7) \equiv 24 \bmod 64$.

If $|x| < 1$, then $7^x \equiv 1 \bmod 16$. If $|x| = \frac{1}{2}$, then $3^x \equiv 5^x \equiv 9 \bmod 16$, while if $|x| < \frac{1}{2}$, then $3^x \equiv 5^x \equiv 1 \bmod 16$. Thus, for $|x| < 1$,

$$f'_{0,7}(x) \equiv \begin{cases} 35 \cdot 9 \cdot 52 + 21 \cdot 9 \cdot 60 + 24 \equiv 32 & \mod 64, \quad \text{if } |x| = \frac{1}{2}, \\ 35 \cdot 1 \cdot 52 + 21 \cdot 1 \cdot 60 + 24 \equiv 32 & \mod 64, \quad \text{if } |x| < \frac{1}{2}, \end{cases}$$

showing that $|f'_{0,7}(x)| = \frac{1}{32}$ if $|x| < 1$. If $|x| = 1$, then we need only calculate modulo 16. We have $L(3) \equiv 4 \bmod 16$, $L(5) \equiv 12 \bmod 16$ and $L(7) \equiv 8 \bmod 16$, while $|x| = 1$ gives $3^x \equiv 3 \bmod 4$ and $5^x \equiv 1 \bmod 4$, so that $f'_{0,7}(x) \equiv 35 \cdot 3 \cdot 4 + 21 \cdot 1 \cdot 12 + 8 \equiv 8 \bmod 16$. Thus $|f'_{0,7}(x)| = \frac{1}{8}$ if $|x| = 1$.

We can easily verify that $|g_{0,7}(x,h)| \leqslant \frac{1}{16}$ for $h \in 2\mathbf{Z}_2$, using Lemma 6. But we will need $g_{0,7}(x,h)$ more accurately for the inequality of Proposition 1. Using Corollary 7 and the previous computations we find that if $h \in 2\mathbf{Z}_2$

$$\frac{3^h - 1 - hL(3)}{h^2} \equiv \frac{5^h - 1 - hL(5)}{h^2} \equiv 8 \mod 64.$$

It is now simple to check that $|g_{0,7}(x,h)| = \frac{1}{32}$ if $x, h \in 2\mathbf{Z}_2$. Similarly we calculate that $|g_{0,7}(x,h)| = \frac{1}{16}$ if $x \in 1 + 2\mathbf{Z}_2$ and $h \in 2\mathbf{Z}_2$. Since $|f_{0,7}(0)| = \frac{1}{64}$ and $|f_{0,7}(1)| = \frac{1}{32}$ the inequality (2) holds in each case giving unique 2-adic integers $u_0 \in 2\mathbf{Z}_2$ and $u_1 \in 1 + 2\mathbf{Z}_2$ such that $f_{0,7}(u_0) = f_{0,7}(u_1) = 0$. The first 50 digits of these zeros are given in the appendix. It follows now from Proposition 2 that

$$|T_2(n,7)| = \begin{cases} |n - u_0|/32, & \text{if } n \text{ is even,} \\ |n - u_1|/8, & \text{if } n \text{ is odd.} \end{cases}$$

4. Explicit Calculations with $p = 3$

For the prime 3 the first interesting case is where $k = 4$. We have $f_{0,4}(x) = -4 + 6 \cdot 4^x + 16^x$, with $f_{0,4}(m) = T_3(2m, 4)$, and $f'_{0,4}(x) = 6 \cdot 4^x L(4) + 16^x L(16)$. It follows from Proposition 4 that $|f'_{0,4}(x)| = \frac{1}{3}$ for all x, and Lemma 6 shows that $|g_{0,4}(x,h)| = \frac{1}{9}$ for all x and h. Now $|f_{0,4}(0)| = \frac{1}{3}$ so that the inequality (2) holds and there is a unique $v_0 \in \mathbf{Z}_3$ such that $f_{0,4}(v_0) = 0$. Since, by Proposition 4, $f'_{0,4}(x) \equiv 6 \bmod 9$ for all x, we may evaluate v_0 by iterating the function $x \mapsto x + f_{0,4}(x)/3$. The first 50 digits of this zero are given in the appendix. Since $16^x = (4^x)^2$ we may write $f_{0,4}(x)$ as a quadratic function of 4^x, which may be factorised to show that $v_0 = L(\sqrt{13} - 3)/L(4)$, where $\sqrt{13}$ denotes that square root of 13 satisfying $\sqrt{13} \equiv 1 \bmod 3$. By Proposition 2, $|f_{0,4}(x)| = |x - v_0|/3$ for all $x \in \mathbf{Z}_3$.

The situation for $f_{1,4}(x) = -4 + 12 \cdot 4^x + 4 \cdot 16^x$, with $f_{1,4}(m) = T_3(2m+1, 4)$, is exactly similar. Again $|f'_{1,4}(x)| = \frac{1}{3}$ and $|g_{1,4}(x,h)| = \frac{1}{9}$ for all x and h, with $|f_{1,4}(0)| = \frac{1}{3}$ so that there is a unique $v_1 \in \mathbf{Z}_3$ such that $f_{1,4}(v_1) = 0$, which may be evaluated by iterating the function $x \mapsto x + f_{1,4}(x)/3$. As before, we may write $f_{1,4}(x)$ as a quadratic in 4^x and we find that $v_1 = L((3 - \sqrt{13})/2)/L(4)$. By Proposition 2, $|f_{1,4}(x)| = |x - v_1|/3$ for all $x \in \mathbf{Z}_3$. Thus

$$v_3(T_3(n,4)) = \begin{cases} 1 + v_3(n - 2v_0), & \text{if } n \text{ is even,} \\ 1 + v_3(n - 2v_1 - 1), & \text{if } n \text{ is odd.} \end{cases}$$

The function $f_{0,5}(x) = 5 - 10 \cdot 4^x - 5 \cdot 16^x + 25^x$ is much more subtle, for $f'_{0,5}$ has a zero in $\mathbf{Z}_3$. In fact the coset $5 + 9\mathbf{Z}_3$ contains two zeros of $f_{0,5}$ and one zero of $f'_{0,5}$.

We have $f'_{0,5}(x) = -10 \cdot 4^x L(4) - 5 \cdot 16^x L(16) + 25^x L(25)$ and, by Proposition 5, $L(4) \equiv 48 \bmod 243$, $L(16) \equiv 96 \bmod 243$, and $L(25) \equiv 132 \bmod 243$. Now the series expansion $y^x = 1 + (y-1)x + (y-1)^2 \binom{x}{2} + \cdots$, where $y \equiv 1 \bmod 3$, shows that, if $x \in 5 + 9\mathbf{Z}_3$,

$$4^x = 4^5 \cdot 4^{x-5} \equiv 4^5(1 + 3(x-5)) \qquad \bmod 81$$

$$\equiv 1 + 75x \qquad \bmod 81.$$

Similarly $16^x \equiv 55 + 60x \bmod 81$ and $25^x \equiv 55 + 42x \bmod 81$. It follows that if $x \in 5 + 9\mathbf{Z}_3$, then

$$f'_{0,5}(x) \equiv -10(1 + 75x)\,48 - 5(55 + 60x)\,96 + (55 + 42x)\,132 \qquad \bmod 243$$

$$\equiv 63 + 36x \qquad \bmod 243.$$

Hence if $x \equiv 14$ or $23 \bmod 27$, then $|f'_{0,5}(x)| = \frac{1}{81}$.

Now Lemma 6 shows that $|g_{0,5}(x,h)| \leqslant \frac{1}{9}$ for all $x, h \in \mathbf{Z}_3$ and it is easy to compute that $|f_{0,5}(14)| = |f_{0,5}(23)| = 3^{-7}$. Proposition 1 and Corollary 3 show that there are unique zeros w_0 and w_1 of $f_{0,5}(x)$ in each of $14 + 27\mathbf{Z}_3$ and $23 + 27\mathbf{Z}_3$. In fact $w_0 = \frac{1}{2}$, for, since $y^x \equiv 1 \bmod 3$ for all $x \in \mathbf{Z}_3$ and $y \in 1 + 3\mathbf{Z}_3$, we have $4^{1/2} = -2$, $16^{1/2} = 4$ and $25^{1/2} = -5$, showing that $f_{0,5}(\frac{1}{2}) = 0$.

It is similarly easy to check that $f'_{0,5}(x)$ has a unique zero in $5 + 27\mathbf{Z}_3$.

Proposition 2 shows that if $x \in 14 + 27\mathbf{Z}_3$, then $|f_{0,5}(x)| = |x - w_0|/81$, and similarly $|f_{0,5}(x)| = |x - w_1|/81$ if $x \in 23 + 27\mathbf{Z}_3$. For other values of x we must calculate separately, estimating 4^x, 16^x and 25^x as above. We find that $|f_{0,5}(x)| = \frac{1}{729}$ if $x \equiv 5 \bmod 27$, $|f_{0,5}(x)| = \frac{1}{81}$ if $x \equiv 2$ or $8 \bmod 9$, and $|f_{0,5}(x)| = \frac{1}{9}$ if $x \equiv 0$ or $1 \bmod 3$.

The function $f_{1,5}(x)$ can be analysed much more simply. We have $|f'_{1,5}(x)| = \frac{1}{3}$ for all $x \in \mathbf{Z}_3$ and there is a unique zero z_0 with $|f_{1,5}(x)| = |x - z_0|/3$ for all $x \in \mathbf{Z}_3$.

Assembling this information, we obtain

PROPOSITION 8. *If* $n \geqslant 5$,

$$v_3(T_3(n,5)) = \begin{cases} 2, & \text{if } n \equiv 0 \text{ or } 2 \bmod 6, \\ 4, & \text{if } n \equiv 4 \text{ or } 16 \bmod 18, \\ 6, & \text{if } n \equiv 10 \bmod 54, \\ v_3(n-1) + 4, & \text{if } n \equiv 28 \bmod 54, \\ v_3(n - 2w_1) + 4, & \text{if } n \equiv 46 \bmod 54, \\ v_3(n - 2z_0 - 1) + 1, & \text{if } n \text{ is odd.} \end{cases}$$

5. The Divisibility of Stirling Numbers

In this section we consider what conclusions can be drawn for the divisibility of the Stirling numbers $S(n, k)$.

Let

$$R_p(n, k) = \sum_{\substack{j=0 \\ p \nmid j}}^{k} (-1)^{k-j} \binom{k}{j} j^n,$$

then $k!\, S(n, k) = T_p(n, k) + R_p(n, k)$. The summand $R_p(n, k)$ is designed to be highly divisible by p. If $v_p(T_p(n, k)) < v_p(R_p(n, k))$, then $v_p(k!\, S(n, k)) = v_p(T_p(n, k))$.

Now clearly $v_p(R_p(n, k)) \geqslant n$.

Conjecture A. If $n \geqslant k$ and p is an odd prime, then

$$v_p(T_p(n, k)) < n.$$

This is clearly equivalent to

Conjecture A′. If $n \geqslant k$ and p is an odd prime, then

$$v_p(k!\, S(n, k)) < n.$$

For $p = 3$ and $k = 5$, Conjecture A may be checked by using Proposition 8. Evaluation of the 3-adic zeros shows that the conjecture holds for $5 \leqslant n < 3^{100}$ (the zeros are given modulo 3^{50} in the Appendix, but the calculations have been extended up to the larger modulus). Beyond this we may argue as follows. Clearly any counterexample must be odd or be congruent to 46 modulo 54. Consider, for example, the possibility of an odd integer satisfying $v_3(T_3(n, 5)) \geqslant n$. It must be at least 3^{100} and satisfy $v_3(n - 2z_0 - 1) \geqslant n - 1$. This would mean that the 3-adic expansion of $2z_0 + 1$ contained at least $n - \log_3(n) - 2 > 3^{100} - 102$ consecutive digits equal to zero. This seems rather unlikely. Davis makes this point, for the case where $p = 2$ and $k = 5$, in [9].

For fixed j, $S(n, n - j)$ is a polynomial function of n, of degree $2j$, which is divisible by $n(n-1)\cdots(n-j)$; see formula (6.26) of [11]. It follows that

$$(n - j)!\, S(n, n - j) = n!\, f_j(n),$$

where f_j is a (rational) polynomial function of degree j. Since $v_p(n!) \geqslant n/(p-1)$ and $v_p(f_j(n))$ cannot grow too rapidly, we can deduce that for each j there can be only a finite number of counterexamples to Conjecture A′ for which $k = n - j$. A detailed analysis shows that there are none at all in the cases $1 \leqslant j \leqslant 4$.

A computer search (of possibly too limited a range) has found no failures of Conjecture A′.

For $p=2$ the corresponding conjectures do not hold. For example, if $n=2^r m+1$, where m is odd, $v_2((n-1)!\,S(n,n-1))=n+r-m+v_2(m!)-2$, so that $v_2((n-1)!\,S(n,n-1))\geqslant n$ if $r\geqslant m+2-v_2(m!)$. A computer search throws up other examples. With $k\leqslant n\leqslant 1200$ there are 167 cases where $v_2(k!\,S(n,k))\geqslant n$. All of these examples have $n-k$ small (at most 15 in the range just mentioned), so it may be reasonable to suppose that, for a fixed k, the analogue when $p=2$ of Conjecture A′ holds for n sufficiently large. This is supported by the results for $k\leqslant 7$ in Section 3.

However in all the cases we know in which $v_2(k!\,S(n,k))\geqslant n$, the value of $v_2(R_2(n,k))$ is sufficiently large that it is nonetheless true that $v_2(k!\,S(n,k))=v_2(T_2(n,k))$. For example, in the case discussed above where m is odd and $k=n-1=2^r m$,

$$R_2(n,n-1)=\sum_{i=0}^{2^{r-1}m}\binom{2^r m}{2i}(2i)^{2^r m+1}.$$

Now $v_2(\binom{2^r m}{j})\geqslant r-v_2(j)$ so that

$$\begin{aligned}v_2\left(\binom{2^r m}{2i}(2i)^{2^r m+1}\right)&\geqslant r-1-v_2(i)+(2^r m+1)(1+v_2(i))\\&=2^r m(1+v_2(i))+r\\&\geqslant 2^r m+r\\&=n+r-1,\qquad \text{for all}\quad i\geqslant 1.\end{aligned}$$

Therefore

$$\begin{aligned}v_2(R_2(n,n-1))&\geqslant n+r-1>n+r-m+v_2(m!)-2\\&=v_2((n-1)!\,S(n,n-1)).\end{aligned}$$

Thus we have no counterexamples to the following conjecture which follows from Conjecture A (or Conjecture A′) for the case where p is odd.

CONJECTURE B. *If $n\geqslant k$ and p is prime, then*

$$v_p(S(n,k))=v_p(T_p(n,k)).$$

We may summarise our conclusions for the divisibility of the Stirling numbers in the following result. Parts 1 and 2 are due to Davis [9].

THEOREM 9. *The following hold for all n less than 2^{100} or 3^{100}, as appropriate, and would follow for all n from Conjecture B.*

(1) *Let u_0 and u_1 be the two 2-adic zeros of $f_{0,5}$. If $n \geq 5$, then*

$$v_2(S(n,5)) = \begin{cases} -1 + v_2(n-u_0), & \text{if } n \text{ is even,} \\ -1 + v_2(n-u_1), & \text{if } n \text{ is odd.} \end{cases}$$

(2) *Let u_0 and u_1 be the two 2-adic zeros of $f_{0,6}$. If $n \geq 6$, then*

$$v_2(S(n,6)) = \begin{cases} -1 + v_2(n-u_0), & \text{if } n \text{ is even,} \\ -1 + v_2(n-u_1), & \text{if } n \text{ is odd.} \end{cases}$$

(3) *Let u_0 and u_1 be the two 2-adic zeros of $f_{0,7}$. If $n \geq 7$, then*

$$v_2(S(n,7)) = \begin{cases} 1 + v_2(n-u_0), & \text{if } n \text{ is even,} \\ -1 + v_2(n-u_1), & \text{if } n \text{ is odd.} \end{cases}$$

(4) *Let v_0 and v_1 be the 3-adic zeros of $f_{0,4}$ and $f_{1,4}$, respectively. If $n \geq 4$, then*

$$v_3(S(n,4)) = \begin{cases} v_3(n-2v_0), & \text{if } n \text{ is even,} \\ v_3(n-2v_1-1), & \text{if } n \text{ is odd.} \end{cases}$$

(5) *Let w_1 be the zero of $f_{0,5}$ in $23+27\mathbf{Z}_3$, and z_0 the zero of $f_{1,5}$. If $n \geq 5$, then*

$$v_3(S(n,5)) = \begin{cases} 1, & \text{if } n \equiv 0 \text{ or } 2 \bmod 6, \\ 3, & \text{if } n \equiv 4 \text{ or } 16 \bmod 18, \\ 5, & \text{if } n \equiv 10 \bmod 54, \\ v_3(n-1)+3, & \text{if } n \equiv 28 \bmod 54, \\ v_3(n-2w_1)+3, & \text{if } n \equiv 46 \bmod 54, \\ v_3(n-2z_0-1), & \text{if } n \text{ is odd.} \end{cases}$$

APPENDIX: NUMERICAL RESULTS

The first 100 digits of the 2-adic zeros of the functions $f_{0,5}$ and $f_{0,6}$ were given in [9]. We reproduce the first 50 digits of these numbers below (in a slightly different format) as well as the first 50 digits of the other 2-adic and 3-adic zeros encountered in Sections 3 and 4. These numbers are written with the least significant digit first. Each number is also given in (conventional) decimal form modulo 2^{50} or 3^{50}. The calculations were performed using, in the first instance, the unix program bc, and then later using the PARI system.

Zeros in $\mathbf{Z}_2$

(1) The two zeros of $f_{0,5}$:

$$00111\ 00100\ 00100\ 01111\ 01110\ 11011\ 11001\ 00010\ 01100\ 10000\ \cdots$$
$$\equiv 42077642494108 \mod 2^{50},$$
$$11111\ 00010\ 01001\ 01001\ 10000\ 10111\ 10000\ 10101\ 10001\ 00110\ \cdots$$
$$\equiv 441627765721375 \mod 2^{50}.$$

(2) The two zeros of $f_{0,6}$:

$$00100\ 10100\ 10001\ 00010\ 00001\ 01100\ 01110\ 00101\ 01101\ 10101\ \cdots$$
$$\equiv 763763515212964 \mod 2^{50},$$
$$10110\ 01001\ 00110\ 11010\ 01001\ 11001\ 11011\ 11010\ 01011\ 01000\ \cdots$$
$$\equiv 99363651433037 \mod 2^{50}.$$

(3) The two zeros of $f_{0,7}$:

$$01110\ 01100\ 01010\ 00010\ 10011\ 00111\ 10111\ 01100\ 01101\ 01111\ \cdots$$
$$\equiv 1079958681430222 \mod 2^{50},$$
$$10110\ 01000\ 00101\ 01110\ 00000\ 10010\ 00111\ 11001\ 11111\ 10001\ \cdots$$
$$\equiv 632902388240461 \mod 2^{50}.$$

Zeros in $\mathbf{Z}_3$

(1) The unique zero of $f_{0,4}$, known as v_0 in Section 4 (recall that $v_0 = L(\sqrt{13}-3)/L(4)$):

$$11000\ 21000\ 11212\ 10122\ 20110\ 00122\ 21201\ 10102\ 22002\ 21222\ \cdots$$
$$\equiv 708156167022899387910400 \mod 3^{50}.$$

(2) The unique zero of $f_{1,4}$, known as v_1 in Section 4 (recall that $v_1 = L((3-\sqrt{13})/2)/L(4)$):

$$10111\ 22011\ 00221\ 20021\ 10001\ 11021\ 12100\ 01012\ 11012\ 12111\ \cdots$$
$$\equiv 368690814514879495244974 \mod 3^{50}.$$

(3) The second zero of $f_{0,5}$, known as w_1 in Section 4 (recall that $w_0 = \frac{1}{2}$ is also a zero):

$$21210\ 00220\ 02002\ 00212\ 01101\ 12210\ 01100\ 22201\ 20022\ 02002\ \cdots$$
$$\equiv 498980261661019908756935 \mod 3^{50}.$$

(4) The unique zero of $f_{1,5}$, known as z_0 in Section 4:

$$10101\ 20221\ 11010\ 11222\ 11212\ 10002\ 10220\ 10112\ 11222\ 02220\ \cdots$$
$$\equiv 233339886936595093155823 \mod 3^{50}.$$

REFERENCES

1. Y. AMICE, "Les Nombres p-adiques," Presses Universitaires de France, Paris, 1975.
2. D. BARSKY, Fonctions k-Lipschitziennes sur un anneau local et polynômes à valeurs entières, *Bull. Soc. Math. France* **101** (1973), 397–411.
3. H. W. BECKER AND J. RIORDAN, The arithmetics of Bell and Stirling numbers, *Amer. J. Math.* **70** (1948), 385–394.
4. L. CARLITZ, A theorem of Glaisher, *Canad. J. Math.* **5** (1953), 306–316.
5. J. W. S. CASSELS, "Local Fields," London Mathematical Society Student Texts, Vol. 3, Cambridge Univ. Press, Cambridge, U.K., 1986.
6. F. CLARKE, Self maps of BU, *Math. Proc. Camb. Phil. Soc.* **89** (1981), 491–500.
7. L. COMTET, "Advanced Combinatorics," D. Reidel, Dordrecht and Boston, 1974.
8. M. C. CRABB AND K. KNAPP, The Hurewicz map on stunted complex projective spaces, *Amer. J. Math.* **110** (1974), 783–809.
9. D. M. DAVIS, Divisibility by 2 of Stirling-like numbers, *Proc. Amer. Math. Soc.* **110** (1990), 597–600.
10. R. GODEMENT, "Cours d'algèbre," Hermann, Paris, 1963.
11. R. L. GRAHAM, D. E. KNUTH, AND O. PATASHNIK, "Concrete Mathematics: A Foundation for Computer Science," Addison–Wesley, Reading, MA, 1989.
12. F. T. HOWARD, Extensions of congruences of Glaisher and Nielsen concerning Stirling numbers, *Fibonacci Q.* **28** (1990), 355–362.
13. F. T. HOWARD, Congruences for the Stirling numbers and associated Stirling numbers, *Acta Arith.* **55** (1990), 29–41.
14. N. KOBLITZ, "p-adic Numbers, p-adic Analysis and Zeta Functions," Springer-Verlag, New York/Heidelberg/Berlin, 1977.
15. Y. H. HARRIS KWONG, Minimum periods of $S(n, k)$ modulo M, *Fibonacci Q.* **27** (1989), 217–221.
16. S. LANG, "Algebraic Number Theory," Addison-Wesley, Reading, MA, 1970.
17. T. LENGYEL, On the divisibility by 2 of the Stirling numbers of the second kind, *Fibonacci Q.* **31** (1993), 597–600.
18. A. T. LUNDELL, Generalized e-invariants and the numbers of James, *Q. J. Math.* **25** (1974), 427–440.
19. A. T. LUNDELL, A divisibility property of Stirling numbers, *J. Number Theory* **10** (1978), 35–54.
20. A. T. LUNDELL, A divisibility property of Stirling numbers, II, preprint (1990).

21. K. MAHLER, "p-adic Numbers and Their Functions," second ed., Cambridge Univ. Press, Cambridge, U.K., 1981.
22. A. NIJENHUIS AND H. S. WILF, Periodicities of partition functions and Stirling numbers modulo p, *J. Number Theory* **25** (1987), 308–312.
23. R. PEELE, Divisibility patterns for some combinatorial sequences, Combinatorics '88, Ravello, Italy, Vol. 2, 1988, pp. 287–294.
24. R. STRASSMANN, Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen, *J. Reine Angew. Math.* **159** (1928), 13–28; 65–66.
25. M. SVED, Divisibility—with Visibility, *Math. Intell.* **10** (1988), 56–64.
26. H. TSUMURA, On some congruences for the Bell numbers and for the Stirling numbers, *J. Number Theory* **38** (1991), 206-211.
27. C. S. WEISMAN, On p-adic differentiability, *J. Number Theory* **9** (1977), 79–86.